ON THE COLLECTION OF INTEGERS THAT INDEX THE FIXED POINTS OF MAPS ON THE SPACE OF RATIONAL FUNCTIONS

CURTIS D. BENNETT AND EDWARD MOSTEIG

Abstract. Given integers s and t, define a function $\phi_{s,t}$ on the space of all formal complex series expansions by $\phi_{s,t}(\sum a_n x^n) = \sum a_{sn+t} x^n$. We define an integer r to be distinguished with respect to (s,t) if r and s are relatively prime and and $r \mid t(1+s+\cdots s^{\mathrm{ord}_r(s)-1})$. The vector space consisting of all rational functions whose Taylor expansions at zero are fixed by $\phi_{s,t}$ was previously classified by constructing a basis that is partially indexed by integers that are distinguished with respect to the pair (s,t). In this paper, we study the properties of the set of distinguished integers with respect to (s,t). In particular, we demonstrate that the set of distinguished integers with respect to (s,t) can be written as a union of infinitely many arithmetic progressions. In addition, we construct another generating set for the collection of rational functions that are fixed by $\phi_{s,t}$ and discuss the relationship between this generating set and the basis that was generated previously.

1. Introduction

Consider the space $\mathfrak{S}$ of all formal series with complex coefficients of the form

$$R(x) = \sum_{n=-\infty}^{\infty} a_n x^n.$$

Let $\mathfrak{R}$ denote the space of rational functions with complex coefficients. The Taylor expansion at $x = 0$ of $R \in \mathfrak{R}$ can be written as a Laurent series, i.e.,

$$R(x) = \sum_{n \gg -\infty} a_n x^n \tag{1.1}$$

where $n \gg -\infty$ denotes the fact that the coefficients vanish for large negative n.

For $s, t \in \mathbb{Z}$, define the map $\phi_{s,t} : \mathfrak{S} \to \mathfrak{S}$ by

$$\phi_{s,t}(\sum a_n x^n) = \sum a_{sn+t} x^n. \tag{1.2}$$

When s is positive, consider the restriction $\phi_{s,t} : \mathfrak{R} \to \mathfrak{R}$. The fixed points of $\phi_{s,t}$ are described in [1] and [5], but these points are parameterized by sequences of integers that are not well understood. The purpose of this paper is shed some light on the situation. Before recalling the results of [5], we need a few preliminary definitions.

Definition 1.1. An integer $r \geq 2$ is called *distinguished* with respect to the pair (s,t) if r and s are relatively prime and and

$$r \mid \beta_{s,t}(\mathrm{ord}_r(s))$$

where

$$\beta_{s,t}(k) = t\left(\frac{s^k - 1}{s - 1}\right)$$

and $\mathrm{ord}_r(s)$ represents the smallest positive integer such that $s^{\mathrm{ord}_r(s)} \equiv 1 \mod r$. We denote the set of integers distinguished with respect to (s,t) by $\Omega(s,t)$.

The description of all the fixed points of $\phi_{s,t}$ requires the notion of *cyclotomic cosets*: given n, $r \in \mathbb{N}$ with $r \geq 1$ such that r and s are relatively prime,

$$C_{s,r,n} = \{s^i n \mod r : i \in \mathbb{Z}\} \tag{1.3}$$

is a finite set called the s-cyclotomic coset of n mod r. Define $\Lambda_{s,r}$ to be a complete collection of coset representatives (all chosen to be less than r); i.e., for all $n \in \mathbb{N}$, there exists a unique $n' \in \Lambda_{s,r}$ such that $C_{s,r,n} = C_{s,r,n'}$. For $r, n \geq 1$, define

$$\psi_{s,t,r,n}(x) = \sum_{j=1}^{\mathrm{ord}_r(s)} \phi_{s,t}^{(j)}\left(\frac{1}{1-\omega_r^n x}\right) = \sum_{j=1}^{\mathrm{ord}_r(s)} \frac{\omega_r^{n\beta_{s,t}(j)}}{1-\omega_r^{ns^j} x}, \tag{1.4}$$

where $\omega_s = e^{2\pi i/s}$ and $\phi_{s,t}^{(j)}$ represents the j-th iterate of the function $\phi_{s,t}$. When $n = 0$, the function $\psi_{s,t,r,n}$ is defined to be $1/(1-x)$. We recall the following result from [5].

Theorem 1.2. *Suppose $s \geq 2$ and $1 \leq t \leq s-2$. The function $1/(1-x)$ together with the collection of all $\psi_{s,t,r,n}$ where r is distinguished with respect to (s,t) and $n \in \Lambda_{s,r}$ is relatively prime to r form a basis for the set of all rational functions that are fixed under the transformation $\phi_{s,t}$.*

Although this theorem provides us with a basis for the space of rational functions fixed by $\phi_{s,t}$, it is somewhat unsatisfactory in that it does not give us a good sense of what it means for an integer r to be distinguished with respect to the pair (s,t). It was shown in [5] that the collection of integers that are distinguished with respect to (s,t) has infinite cardinality, but that is pretty much the limit of what was discussed. In this paper, we explore one of the questions posed in [5], namely, whether or not $\Omega(s,t)$ is a union of arithmetic sequences. We begin by examining this problem in Section 2 and show, among other results that, indeed, $\Omega(3,1)$ is an infinite union of arithmetic sequences. In Section 3, we generalize the results of Section 2 to the case when working with an arbitrary pair (s,t). In particular, we show that $\Omega(s,t)$ is a union of arithmetic sequences, and then we provide conditions for when multiples of a particular form of a fixed integer are distinguished with respect to (s,t).

In the course of studying distinguished integers with respect to a given pair (s,t), another collection of rational functions that span that space of functions fixed by $\phi_{s,t}$ was discovered. In Section 4, we describe this spanning set and discuss its relationship to the collection of functions of the form $\psi_{s,t,r,n}$.

2. Distinguished with Respect to $(3,1)$

In this section, we will examine the special case of $(3,1)$-distinguished integers. We begin with this case, as it is the simplest interesting case. Moreover, the experimental data in this case suggests a number of avenues for investigation. From the analysis of the $(3,1)$ case, we can discover several interesting propositions, some of which we generalize in the next section.

The table below shows all the integers up to 204 that are distinguished (shaded) with respect to $(3, 1)$.

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108
109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132
133	134	135	136	137	138	139	140	141	142	143	144
145	146	147	148	149	150	151	152	153	154	155	156
157	158	159	160	161	162	163	164	165	166	167	168
169	170	171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190	191	192
193	194	195	196	197	198	199	200	201	202	203	204

Upon examining this table, it seems rather likely that all positive integers that are congruent to either 1 or 5 modulo 6 must be distinguished with respect to $(3, 1)$. Moreover, it appears that all positive integers congruent to 4, 10, 14, or 20 modulo 24 must be $(3, 1)$-distinguished. In fact, both statements are true and are mentioned in [5], and below we will provide proofs. Our general methods only yield the case of 10 modulo 60 and 14 modulo 88 rather than modulo 24. To obtain the proofs for 10 and 14 modulo 24, we use quadratic reciprocity. One would hope for simpler proofs of these last two cases, and the interested reader is encouraged to look for such proofs.

Of the remaining distinguished integers in the table above, 40 is the smallest. Again, the pattern seems promising. Multiply the previous modulus by four to obtain 96. Jumping to conclusions, it seems likely that all positive integers congruent to 40 modulo 96 must be distinguished. In fact, 40, 136, 232, 328, 424, and 520 are all distinguished with respect to $(3, 1)$, but 616 is not! This surprising gap leads to some interesting questions. In light of this example, it is not clear whether the collection of all integers that are distinguished with respect to $(3, 1)$ can be written as a (possibly infinite) union of congruence classes, and we now turn to answer this question.

We begin by establishing that odd positive integers relatively prime to 6 are $(3, 1)$-distinguished.

Lemma 2.1. *Every integer congruent to 1 or 5 modulo 6 must be distinguished with respect to* $(3, 1)$.

Proof. Suppose r is congruent to 1 or 5 modulo 6; that is, r is relatively prime to 6. By definition, $3^{\mathrm{ord}_r(3)} \equiv 1 \mod r$, and so $r \mid 3^{\mathrm{ord}_r(3)} - 1$. Now, $3^{\mathrm{ord}_r(3)} - 1$ is even and r is odd, and so $r \mid \frac{3^{\mathrm{ord}_r(3)}-1}{3-1}$. □

It is a bit trickier to justify that positive integers in the equivalence classes modulo 24 containing 4 and 20 are distinguished with respect to $(3, 1)$. Since

these equivalence classes consist solely of even integers, we must employ a different argument. To begin, we note the following result.

Lemma 2.2. *Let r be a positive integer that is relatively prime to 3. Then r is distinguished with respect to $(3,1)$ if and only if $ord_r(3) = ord_{2r}(3)$.*

Proof. If r is distinguished with respect to $(3,1)$, then $r \mid (3^{\mathrm{ord}_r(3)} - 1)/(3-1)$, and so $3^{\mathrm{ord}_r(3)} \equiv 1 \mod 2r$. Thus $\mathrm{ord}_r(3) \geq \mathrm{ord}_{2r}(3)$, and since the reverse inequality always holds, $\mathrm{ord}_r(3) = \mathrm{ord}_{2r}(3)$.

Conversely, suppose $\mathrm{ord}_r(3) = \mathrm{ord}_{2r}(3)$. Since $3^{\mathrm{ord}_{2r}(3)} \equiv 1 \mod 2r$, it follows that $3^{\mathrm{ord}_r(3)} \equiv 1 \mod 2r$, and so $2r \mid 3^{\mathrm{ord}_r(3)} - 1$, in which case $r \mid (3^{\mathrm{ord}_r(3)} - 1)/(3-1)$. □

We note that if m and n are relatively prime, then $\mathrm{ord}_{mn}(a) = \mathrm{lcm}(\mathrm{ord}_m(a), \mathrm{ord}_n(a))$ (which follows as the group of multiplicative units modulo mn is a direct product of the group of units modulo m and the group of units modulo n). As a result, by writing $r = 2^t k$ with $\gcd(2,k) = 1$, we see that the validity of the equation $\mathrm{ord}_r(3) = \mathrm{ord}_{2r}(3)$ hinges on the relationship between $\mathrm{ord}_{2^t}(3)$, $\mathrm{ord}_{2^{t+1}}(3)$ and $\mathrm{ord}_k(3)$. We begin our more general analysis by examining the relationship between the first two of these quantities.

Proposition 2.3. *For $\ell \geq 3$, $ord_{2^\ell}(3) = 2^{\ell-2}$.*

Proof. We will prove that $3^{2^\ell} - 1 \equiv 2^{\ell+2} \mod 2^{\ell+3}$ by induction, from which the result follows. It is easily verified that this holds for $\ell = 3$, and so we assume $3^{2^\ell} - 1 \equiv 2^{\ell+2} \mod 2^{\ell+3}$ for a particular value of ℓ. From this, it follows that for some $q \in \mathbb{N}$, $3^{2^\ell} - 1 - 2^{\ell+2} = 2^{\ell+3}q$. Moreover, for all $\ell \geq 1$, $3^{2^\ell} \equiv 1 \mod 4$, and so $3^{2^\ell} + 1 \equiv 2 \mod 4$; thus $3^{2^\ell} + 1 = 4q' + 2$ for some $q' \in \mathbb{N}$. Thus, $3^{2^{\ell+1}} - 1 = (3^{2^\ell} + 1)(3^{2^\ell} - 1) = (4q'+2)(2^{\ell+2} + 2^{\ell+3}q) = 2^{\ell+3}(1+q)(1+2q)$, and so $3^{2^{\ell+1}} - 1 \equiv 2^{\ell+3} \mod 2^{\ell+4}$. □

We note that $\mathrm{ord}_2(3) = 1$ and $\mathrm{ord}_4(3) = 2 = \mathrm{ord}_8(3)$; from the latter we have that 4 is necessarily $(3,1)$-distinguished. The following lemma generalizes the case of 4 to numbers of the form $2^\ell k$ with $\gcd(6,k) = 1$.

Lemma 2.4. *Given a positive integer $r = 2^\ell k$ such that $\ell \geq 3$ and $\gcd(k,6) = 1$, r is distinguished with respect to $(3,1)$ if and only if $2^{\ell-1} \mid ord_k(3)$. Moreover, if $r = 2k$ with $\gcd(k,6) = 1$, then r is $(3,1)$-distinguished if and only if $2 \mid ord_k(3)$, and if $r = 4k$ with $\gcd(k,6) = 1$, then r $(3,1)$-distinguished.*

Proof. By Lemma 2.2, r is distinguished with respect to $(3,1)$ if and only if $\mathrm{ord}_r(3) = \mathrm{ord}_{2r}(3)$. If r is of the form $r = 2^\ell k$ such that $\ell \geq 3$ and $\gcd(k,6) = 1$, then $\mathrm{ord}_r(3) = \mathrm{lcm}(\mathrm{ord}_{2^\ell}(s), \mathrm{ord}_k(3))$. Moreover, $\mathrm{ord}_{2r}(3) = \mathrm{lcm}(\mathrm{ord}_{2^{\ell+1}}(s), \mathrm{ord}_k(3))$ and so r is distinguished with respect to $(3,1)$ if and only if $\mathrm{lcm}(\mathrm{ord}_{2^\ell}(3), \mathrm{ord}_k(3)) = \mathrm{lcm}(\mathrm{ord}_{2^{\ell+1}}(3), \mathrm{ord}_k(3))$. Since $\mathrm{ord}_{2^{\ell+1}}(3) = 2 \cdot \mathrm{ord}_{2^\ell}(3)$, this condition holds whenever $\mathrm{ord}_{2^{\ell+1}}(3) \mid \mathrm{ord}_k(3)$. By Proposition 2.3, this is equivalent to $2^{\ell-1} \mid \mathrm{ord}_k(3)$.

For the other two cases, we note that if $r = 2k$ with $\gcd(6,k) = 1$, then $\mathrm{ord}_r(3) = \mathrm{ord}_k(3)$, while $\mathrm{ord}_{2r}(3) = \mathrm{lcm}(2, \mathrm{ord}_k(3))$ so that we have equality if and only if $\mathrm{ord}_k(3)$ is even. Alternatively, if $r = 4k$ with $\gcd(6,k) = 1$, then $\mathrm{ord}_r(3) = \mathrm{lcm}(2, \mathrm{ord}_k(3))$, while $\mathrm{ord}_{2r}(3) = \mathrm{lcm}(2, \mathrm{ord}_k(3))$ as $\mathrm{ord}_8(3) = 2 = \mathrm{ord}_4(3)$. □

Since any number r congruent to 4 or 20 modulo 24 is of the form $r = 4k$ where $\gcd(6, k) = 1$, the above lemma implies that all such numbers are $(3, 1)$-distinguished. Sadly, the appearances of arithmetic series 10 and 14 modulo 24 in our chart are still hard to explain.

The following results answer the original question concerning whether all the distinguished integers with respect to $(3, 1)$ can be written as an infinite union of arithmetic sequences.

Corollary 2.5. *Suppose r is $(3, 1)$-distinguished. Then all integers congruent to r or $5r$ modulo $6r$ are also $(3, 1)$-distinguished.*

Proof. Suppose r is $(3, 1)$ distinguished, and write $r = 2^t k$ where $\gcd(6, k) = 1$. It follows from Lemma 2.2 that $\mathrm{ord}_r(3) = \mathrm{ord}_{2r}(3)$. This implies that

$$\mathrm{lcm}(\mathrm{ord}_{2^t}(3), \mathrm{ord}_k(3)) = \mathrm{lcm}(\mathrm{ord}_{2^{t+1}}(3), \mathrm{ord}_k(3)).$$

Suppose $r' = r + 6rm$, for some integer m. Then

$$\begin{aligned} \mathrm{ord}_{r'}(3) &= \mathrm{ord}_{r+6rm}(3) \\ &= \mathrm{ord}_{2^t k(1+6m)}(3) \\ &= \mathrm{lcm}(\mathrm{ord}_{2^t}(3), \mathrm{ord}_{k(1+6m)}(3)). \end{aligned}$$

Similarly, $\mathrm{ord}_{2r'}(3) = \mathrm{lcm}(\mathrm{ord}_{2^{t+1}}(3), \mathrm{ord}_{k(1+6m)}(3))$. Note that $\mathrm{ord}_k(3)$ divides $\mathrm{ord}_{k(1+6m)}(3)$. However, if $\mathrm{lcm}(x, z) = \mathrm{lcm}(y, z)$, then it must be the case that $\mathrm{lcm}(x, za) = \mathrm{lcm}(y, za)$ when $x, y, z, a \in \mathbb{Z}$. Consequently, letting $x = \mathrm{ord}_{2^t}(3)$, $y = \mathrm{ord}_{2^{t+1}}(3)$, $z = \mathrm{ord}_k(3)$ and $za = \mathrm{ord}_{k(1+6m)}(3)$, we have that $\mathrm{ord}_{r'}(3) = \mathrm{ord}_{2r'}(3)$ so that r' is $(3, 1)$-distinguished. For the case of $5r$ modulo $6r$, we note that the only change in the above is that $1+6m$ is replaced by $5+6m$. Thus if $r' = 5r+6mr$ for some $m \in \mathbb{N}$, then r' is $(3, 1)$ distinguished too. □

We could have used Lemma 2.4 and a case-by-case analysis for this, but the above argument is both more elegant and more easily generalized. Note that since 10 is $(3, 1)$-distinguished, Corollary 2.5 implies that if $r \equiv 10 \mod 60$ then r is also $(3, 1)$-distinguished. Similarly, we know that integers congruent to 14 modulo 84 are $(3, 1)$-distinguished. However, neither of these quickly leads to an argument for 10 or 14 modulo 24. On the other hand, we do obtain the following result:

Corollary 2.6. *The set of all $(3, 1)$-distinguished integers can be written as an infinite union of arithmetic progressions.*

Proof. By Corollary 2.5 every $(3, 1)$-distinguished integer r lies in the arithmetic progression $(r + 6rm)_{m=1}^{\infty}$. □

This corollary answers our initial question, but as our difficulty with 10 and 14 show, the answer is not entirely satisfactory. For completeness, we will justify that all positive integers congruent to 10 modulo 24 are $(3, 1)$-distinguished. The proof for 14 is similar.

Proposition 2.7. *Suppose $r \equiv 10 \mod 24$ where $r > 0$. Then r is $(3, 1)$-distinguished.*

Proof. By Lemma 2.2 we need to show that $\mathrm{ord}_r(3) = \mathrm{ord}_{2r}(3)$. Writing $r = 10 + 24k$ where k is a nonnegative integer, this corresponds to showing

$$\mathrm{ord}_{10+24k}(3) = \mathrm{lcm}(\mathrm{ord}_2(3), \mathrm{ord}_{5+12k}(3)) = \mathrm{ord}_{5+12k}(3)$$

is equal to

$$\mathrm{ord}_{20+48k}(3) = \mathrm{lcm}(\mathrm{ord}_4(3), \mathrm{ord}_{5+12k}(3)) = \mathrm{lcm}(2, \mathrm{ord}_{5+12k}(3)).$$

This follows if and only if $\mathrm{ord}_{5+12k}(3)$ is even. Consequently, we simply need to show that $3^{2n+1} \not\equiv 1 \mod 5+12k$ for any n. As $3(2+4k) \equiv 1 \mod 5+12k$, this corresponds to showing that $3^{2n} = (3^n)^2 \not\equiv 2+4k \mod 5+12k$ for any n. Thus the result follows if we show that $2+4k$ is not a square modulo $5+12k$. We turn to quadratic reciprocity for this result. Recall that if a is a square mod b, then the Jacobi symbol $\left(\frac{a}{b}\right) = 1$. Using the algebra of Jacobi symbols (see [4], for example),

$$\begin{aligned}\left(\frac{2+4k}{5+12k}\right) &= \left(\frac{2}{5+12k}\right)\left(\frac{1+2k}{5+12k}\right) \\ &= (-1)^{((5+12k)^2-1)/8}\left(\frac{1+2k}{5+12k}\right) \\ &= (-1)^{k+1}\left(\frac{1+2k}{5+12k}\right),\end{aligned}$$

and

$$\begin{aligned}\left(\frac{5+12k}{1+2k}\right) &= \left(\frac{-1}{1+2k}\right) \\ &= (-1)^k.\end{aligned}$$

By quadratic reciprocity,

$$\begin{aligned}\left(\frac{1+2k}{5+12k}\right)\left(\frac{5+12k}{1+2k}\right) &= (-1)^{((1+2k)-1)((5+12k)-1)/4} \\ &= 1.\end{aligned}$$

Putting these together we obtain

$$\left(\frac{2+4k}{5+12k}\right) = (-1)^{k+1}(-1)^k = -1.$$

implying that $2+4k$ is not a square modulo $5+12k$. Consequently, $\mathrm{ord}_{5+12k}(3)$ is even as desired. Hence r is $(3,1)$-distinguished. □

We note that trying to employ a similar argument for 40 modulo 96, one runs into the problem of trying to show that $(2+4k)^2$ is not a square modulo $5+12k$, which is clearly ridiculous.

3. Distinguished with Respect to (s,t)

In this section we analyze the general case. As we shall see, the (s,t) case is more complicated than the $(3,1)$ case, in part because $s-1$ can be composite. This leads to potential difficulties in calculating $\mathrm{ord}_r(s)$. On the bright side, however, allowing $t \neq 1$ can sometimes make it easier for a number r to be distinguished. We begin this section by examining the role of t.

Lemma 3.1. *Let $r \geq 2$ be relatively prime to s. If r is distinguished with respect to (s,t), then r is distinguished with respect to $(s, \gcd(t, s-1))$.*

Proof. Note that $s^{\mathrm{ord}_r(s)} - 1 = (s-1)(1+s+\cdots+s^{\mathrm{ord}_r(s)-1})$, and so $r \mid (s-1)(1+s+\cdots+s^{\mathrm{ord}_r(s)-1})$. Since r is distinguished with respect to (s,t), it follows that $r \mid t(1+s+\cdots+s^{\mathrm{ord}_r(s)-1})$. Thus, $r \mid \gcd(t, s-1)(1+s+\cdots+s^{\mathrm{ord}_r(s)-1})$. □

We now generalize Lemma 2.2.

Proposition 3.2. *Let $r \geq 2$ be relatively prime to s. Then r is distinguished with respect to (s,t) if and only if $ord_r(s) = ord_{gr}(s)$ where*

$$g = \frac{s-1}{\gcd(s-1,t)}. \tag{3.1}$$

Proof. If r is distinguished with respect to (s,t), then by Lemma 3.1, r is distinguished with respect to $(s, \gcd(t, s-1))$, and so $(s-1)r \mid \gcd(s-1,t)(s^{\mathrm{ord}_r(s)}-1)$. From this, we see $gr \mid s^{\mathrm{ord}_r(s)} - 1$, and so $s^{\mathrm{ord}_r(s)} \equiv 1 \mod gr$. Thus $\mathrm{ord}_r(s) \geq \mathrm{ord}_{gr}(s)$, and since the reverse inequality always holds, $\mathrm{ord}_r(s) = \mathrm{ord}_{gr}(s)$.

Conversely, suppose $\mathrm{ord}_r(s) = \mathrm{ord}_{gr}(s)$. Since $s^{\mathrm{ord}_{gr}(s)} \equiv 1 \mod gr$, it follows that $s^{\mathrm{ord}_r(s)} \equiv 1 \mod gr$, and so $gr \mid s^{\mathrm{ord}_r(s)} - 1$. From this, it follows that $r \mid \gcd(s-1,t)(s^{\mathrm{ord}_r(s)}-1)/(s-1)$, and so $r \mid t(s^{\mathrm{ord}_r(s)}-1)/(s-1)$. □

We now have the following corollary:

Corollary 3.3. *If $\gcd(s-1,t) \mid \gcd(s-1,t')$ (in particular, if $t \mid t'$), then r is distinguished with respect to (s,t') whenever r is distinguished with respect to (s,t).*

In the $(3,1)$ case, we were fortunate that $s-1$ was prime and $g = 1$, which simplified our work. We now turn to generalizing the second part of Lemma 2.4, and afterwards, we shall then generalize its first part.

Proposition 3.4. *Let $p_1, \ldots, p_n$ be the prime divisors of $g = p_1^{j_1} \ldots p_n^{j_n}$. For $r \in \mathbb{Z}$ with $r = p_1^{m_1} \ldots p_n^{m_n} k$ with $\gcd(k,g) = 1$. If $ord_{p_i^{m_i+j_i}}(s)$ divides $ord_r(s)$ for $i = 1, \ldots, n$, then r is (s,t)-distinguished. In particular, if $ord_{p_i^{m_i+j_i}}(s)$ divides $ord_k(s)$, then r (and k) are (s,t)-distinguished.*

Proof. Given r as above, we calculate $\mathrm{ord}_{gr}(s)$. Using prime factorizations, we have

$$\mathrm{ord}_{gk}(s) \quad = \quad \mathrm{lcm}(\mathrm{ord}_{p_1^{m_1+j_1}}(s), \ldots, \mathrm{ord}_{p_n^{m_n+j_n}}(s), \mathrm{ord}_k(s)).$$

Since $k|r$ implies $\mathrm{ord}_k(s)|\mathrm{ord}_r(s)$, it follows that $\mathrm{ord}_{gr}(s) \leq \mathrm{ord}_r(s)$. However, since the latter divides the former, we must have $\mathrm{ord}_{gr}(s) = \mathrm{ord}_r(s)$. Consequently by Proposition 3.2, r is (s,t)-distinguished. □

There are now two basic possibilities for how r can be (s,t)-distinguished. First, if $\mathrm{ord}_{p_i^{m_i+j_i}}(s) = \mathrm{ord}_{p_i^{m_i}}(s)$ then p_i imposes no restriction on k. This is what happened in the $4k$ case for $(3,1)$ as $\mathrm{ord}_4(3) = \mathrm{ord}_8(3)$ (it also occurs in the 1 and 5 modulo 6 cases). Alternatively, if $\mathrm{ord}_{p_i^{m_i+j_i}}(s) > \mathrm{ord}_{p_i^{m_i}}(s)$ then it is necessary that $\mathrm{ord}_{r/p_i^{m_i}}(s)$ is a multiple of $\mathrm{ord}_{p_i^{m_i+j_i}}(s)$. In the $(3,1)$ case, this reduced to $\mathrm{ord}_k(3)$ (in the $r = 2k$ case), as $s - 1 = 2$.

Note that if k is relatively prime to gs, then k is necessarily (s,t)-distinguished since $\mathrm{ord}_{gk}(s) = \mathrm{lcm}(\mathrm{ord}_g(s), \mathrm{ord}_k(s))$, and $g|(s-1)$ implies $\mathrm{ord}_g(s) = 1$. In the remainder of this section, we analyze what multiples of k are (s,t)-distinguished in this case. The following lemma, which follows from Proposition 3.4, allows us to reduce to considering $\mathrm{ord}_{p^\ell}(s)$ and its relationship to $\mathrm{ord}_k(s)$.

Lemma 3.5. *Let $g = p_1^{j_1} \ldots p_n^{j_n}$ be defined as in Proposition 3.2 with each p_i prime, $\bar{g} = p_1 \ldots p_n$ and let $r = p_1^{t_1} \ldots p_n^{t_n} k$ with $\gcd(gs,k) = 1$. Then r is distinguished if and only if for each $i = 1, \ldots, n$ either*

(1) $ord_{p_i^{j_i+t_i}}(s) = ord_{p_i^{t_i}}(s)$ *or*
(2) $ord_{p_i^{j_i+t_i}}(s)$ *divides* $ord_k(s)$.

Similar to what was done in the $(3,1)$ case, Proposition 3.4 allows us to create congruence classes of (s,t)-distinguished positive integers.

Proposition 3.6. *Suppose r is (s,t)-distinguished with g as defined in equation (3.1). Let $g = p_1^{j_1} \dots p_n^{j_n}$ be the prime factorization of g, and set $\bar{g} = p_1 \dots p_n$. Suppose*

$$r' \equiv br \mod \bar{g}rs$$

with $\gcd(b, \bar{g}s) = 1$*, then r' is (s,t)-distinguished.*

Proof. Since r is (s,t)-distinguished, by Proposition 3.2 we have

$$\mathrm{ord}_{gr}(s) = \mathrm{ord}_r(s).$$

Suppose $r = \gamma k$ where $\gcd(k,g) = 1$ and any prime dividing γ divides g. Since $r' = br + \bar{g}rsc = \gamma k(b + \bar{g}sc)$ for some integer c and $\gcd(\gamma, k(b+\bar{g}sc)) = 1$, it follows that

$$\mathrm{ord}_{r'}(s) = \mathrm{lcm}(\mathrm{ord}_\gamma(s), \mathrm{ord}_{k(b+\bar{g}sc)}(s)).$$

Similarly,

$$\mathrm{ord}_{gr'}(s) = \mathrm{lcm}(\mathrm{ord}_{g\gamma}(s), \mathrm{ord}_{k(b+\bar{g}sc)}(s)).$$

By hypothesis, however,

$$\mathrm{lcm}(\mathrm{ord}_\gamma(s), \mathrm{ord}_k(s)) = \mathrm{ord}_r(s) = \mathrm{ord}_{gr}(s) = \mathrm{lcm}(\mathrm{ord}_{g\gamma}(s), \mathrm{ord}_k(s)).$$

Since $\mathrm{ord}_k(s)$ divides $\mathrm{ord}_{k(b+\bar{g}sc)}(s)$, it follows that the above implies

$$\mathrm{lcm}(\mathrm{ord}_\gamma(s), \mathrm{ord}_{k(b+\bar{g}sc)}(s)) = \mathrm{lcm}(\mathrm{ord}_{g\gamma}(s), \mathrm{ord}_{k(b+\bar{g}sc)}(s))$$

implying $\mathrm{ord}_{r'}(s) = \mathrm{ord}_{gr'}(s)$. Proposition 3.2 then implies r' is (s,t)-distinguished as desired. □

This allows us to generalize Corollary 2.6 to the (s,t) case.

Corollary 3.7. *The set of all (s,t)-distinguished integers can be written as an infinite union of arithmetic progressions.*

Applying Proposition 3.6 to the case $r = 10$ for $(s,t) = (3,1)$, we obtain that every term in the arithmetic progression $(10 + 60m)_{m=1}^\infty$ is $(3,1)$-distinguished. We note that this does not contain all $(3,1)$-distinguished arithmetic progressions that include 10. In particular, in Proposition 2.7 we showed that the progression $(10+24m)_{m=1}^\infty$ is $(3,1)$-distinguished. An interesting question is whether for a given α, one could determine all "minimal" μ such that the progression $(\alpha + \mu m)_{m=1}^\infty$ is (s,t)-distinguished.

Proposition 3.6 generalize the argument that 40 lies in an arithmetic sequence of $(3,1)$-distinguished integers. The prime divisor 5 played an important role in the argument for 40. Looking at the chart of $(3,1)$-distinguished integers, we see that 5, 10, 20, and 40 are all $(3,1)$-distinguished, but that $2^t 5$ is not for any $t > 3$. This seems curious. Looking at 7, we note that 7, 14, and 28 are distinguished, but again $2^t 7$ does not seem to be distinguished if $t > 2$. One might be tempted to conjecture that for each prime $p > 3$ there exists a t_0 such that $2^t p$ is $(3,1)$-distinguished for $t < t_0$ but is not distinguished if $t \geq t_0$. However, 11 and 44 are $(3,1)$-distinguished, but 22 is not. In the remainder of the section, we analyze this phenomenon.

We now generalize Proposition 2.3 and the first part of Lemma 2.4.

Proposition 3.8. *Let p be a prime that does not divide s. For $\ell \geq 1$, define $\lambda(\ell, p, s) = ord_{p^{\ell+1}}(s)/ord_{p^\ell}(s)$. Then we have the following.*

(a) *For $\ell \geq 1$, $\lambda(\ell, p, s) \mid p$.*
(b) *For $\ell \gg 0$, $\lambda(\ell, p, s) = p$.*

Proof. Since by definition, $s^{\mathrm{ord}_{p^\ell}(s)} \equiv 1 \mod p^\ell$, it follows that for any non-negative integer i, $s^{i\cdot\mathrm{ord}_{p^\ell}(s)} \equiv 1 \mod p^\ell$, and so $p \mid \sum_{i=0}^{p-1} s^{i\cdot\mathrm{ord}_{p^\ell}(s)}$. By definition, $p^\ell \mid \left(s^{\mathrm{ord}_{p^\ell}(s)} - 1\right)$, and since $s^{p\cdot\mathrm{ord}_{p^\ell}(s)} - 1 = \left(s^{\mathrm{ord}_{p^\ell}(s)} - 1\right)\left(\sum_{i=0}^{p-1} s^{i\mathrm{ord}_{p^\ell}(s)}\right)$, we have $s^{p\cdot\mathrm{ord}_{p^\ell}(s)} s \equiv 1 \mod p^{\ell+1}$. However, by definition, $\mathrm{ord}_{p^{\ell+1}}(s)$ is the smallest exponent such that $s^{\mathrm{ord}_{p^{\ell+1}}(s)} \equiv 1 \mod p^{\ell+1}$, and so $\mathrm{ord}_{p^{\ell+1}}(s) \mid p\cdot\mathrm{ord}_{p^\ell}(s)$. Thus,

$$\lambda(\ell, p, s) \mid p. \tag{3.2}$$

For any positive integer m and prime p, we define the valuation $\nu_p : \mathbb{N}^+ \to \mathbb{N}$ by $\nu_p(m) = j$ where m can be factored as $m = p^j n$ such that n is not divisible by p. Define $\delta_\ell = \nu_p\left(s^{\mathrm{ord}_{p^\ell}(s)} - 1\right) - \ell$. By definition, $p^\ell \mid s^{\mathrm{ord}_{p^\ell}(s)} - 1$, and so $\delta_\ell \geq 0$. Note that

$$s^{\mathrm{ord}_{p^{\ell+1}}(s)} - 1 \quad = \quad s^{\lambda(\ell,p,s)\mathrm{ord}_{p^\ell}(s)} - 1 = (s^{\mathrm{ord}_{p^\ell}(s)} - 1)\left(\sum_{i=0}^{\lambda(\ell,p,s)-1} s^{i\cdot\mathrm{ord}_{p^\ell}(s)}\right),$$

and so

$$\begin{aligned}\delta_\ell - \delta_{\ell+1} &= 1 + \nu_p(s^{\mathrm{ord}_{p^\ell}(s)} - 1) - \nu_p\left(s^{\mathrm{ord}_{p^{\ell+1}}(s)} - 1\right) \\ &= 1 - \nu_p\left(\sum_{i=0}^{\lambda(\ell,p,s)-1} s^{i\cdot\mathrm{ord}_{p^\ell}(s)}\right).\end{aligned}$$

Since $s^{\mathrm{ord}_{p^\ell}(s)} \equiv 1 \mod p^\ell$,

$$\sum_{i=0}^{\lambda(\ell,p,s)-1} s^{i\cdot\mathrm{ord}_{p^\ell}(s)} \equiv \lambda(\ell, p, s) \mod p^\ell. \tag{3.3}$$

and since $\lambda(\ell, p, s) \mid p$, the summation $\sum_{i=0}^{\lambda(\ell,p,s)-1} s^{i\cdot\mathrm{ord}_{p^\ell}(s)}$ is not divisible by p^2 whenever $\ell > 1$, in which case

$$\nu_p\left(\sum_{i=0}^{\lambda(\ell,p,s)-1} s^{i\cdot\mathrm{ord}_{p^\ell}(s)}\right) \leq 1.$$

Thus, $\delta_\ell \geq \delta_{\ell+1}$ for $\ell > 1$, and so the sequence $\{\delta_i\}$ must stabilize; that is, $\delta_\ell = \delta_{\ell+1}$ for $\ell \gg 0$, and so

$$\nu_p\left(\sum_{i=0}^{\lambda(\ell,p,s)-1} s^{i\cdot\mathrm{ord}_{p^\ell}(s)}\right) = 1.$$

Combining this with (3.3), it follows that $\lambda(\ell, p, s) = p$. □

In light of this result, it behooves us to define the stabilization point.

Definition 3.9. Let s be a positive integer not divisible by the prime p. Define $\alpha_{s,p}$ to be the smallest integer such that for any $\ell \geq \alpha_{s,p}$, $\lambda(\ell, p, s) = p$.

In the cases of interest to us, the prime p divides g and hence $s-1$. In this case, we can say more about $\lambda(\ell,p,s)$. In particular, if $p=2$ and $\nu_p(\mathrm{ord}_{p^\ell}(s))>1$, then we shall see $\lambda(\ell,p,s)=2$. Similarly, if $p>2$ is prime, then $\lambda(\ell,p,s)=p$ if $\nu_p(\mathrm{ord}_{p^\ell}(s))\geq 1$. That is, once the p part of the p^ℓ-order of s is p (or 4 if $p=2$), then the order increases by a factor of p each time the power of the modulus increases by 1. Consequently, for primes greater than 2, if we know $\alpha_{s,p}$, we can easily determine $\nu_{p^\ell}(s)$ for all ℓ. We prove this in the remainder of the section.

Lemma 3.10. *If $\lambda(\ell,p,s)=p$ for some $\ell\geq 2$ then $\lambda(m,p,s)=p$ for all $m\geq\ell$.*

Proof. Let $t=\nu_p(\mathrm{ord}_{p^\ell}(s))$. Then we can write $\mathrm{ord}_{p^\ell}(s)$ as xp^t (where $\gcd(x,p)=1$). We now have

$$s^{xp^t} \equiv 1 \mod p^\ell, \tag{3.4}$$

$$s^{xp^t} \not\equiv 1 \mod p^{\ell+1}. \quad \text{and} \tag{3.5}$$

$$s^{xp^{t+1}} \equiv 1 \mod p^{\ell+1}, \tag{3.6}$$

with the last two coming from our assumption that $\lambda(\ell,p,s)=p$.

Equations (3.4) and (3.5) imply $s^{xp^t}-1\equiv yp^\ell \mod p^{\ell+1}$ for some y relatively prime to p. We then have

$$s^{xp^{t+1}}-1=\left(s^{xp^t}-1\right)\left(1+s^{xp^t}+s^{2xp^t}+\cdots+s^{(p-1)xp^t}\right).$$

Therefore

$$\begin{aligned}\nu_p\left(s^{xp^{t+1}}-1\right) &= \nu_p\left(s^{xp^t}-1\right)+\nu_p\left(1+s^{xp^t}+s^{2xp^t}+\cdots+s^{(p-1)xp^t}\right)\\ &= \ell+\nu_p\left(1+s^{xp^t}+(s^{xp^t})^2+\cdots+(s^{xp^t})^{p-1}\right)\\ &= \ell+1.\end{aligned}$$

The second equality holds by equations (3.4) and (3.5). The last equality holds because (3.4) implies each of the p terms is congruent to 1 modulo p^2 (since $\ell\geq 2$). Hence $p^{\ell+2}$ does not divide $s^{xp^{t+1}}-1$ and Proposition 3.8 implies $\lambda(\ell+1,p,s)=p$. By induction $\lambda(m,p,s)=p$ for all $m\geq\ell$. □

In the above proof, the requirement that $\ell\geq 2$ was only used in arguing that $\nu_p\left(1+s^{xp^t}+\cdots+s^{(p-1)xp^t}\right)=1$. If $\ell=1$, we have only that this term is congruent to p modulo p, and thus might be 0 modulo p^2 or p^3, etc. On the other hand, if we knew further that $s=1+py$ for some integer y, by the binomial theorem

$$s^p-1=(1+py)^p-1=\sum_{k=1}^{p}\binom{p}{k}(py)^k.$$

Since $\binom{p}{k}$ is divisibly by p for $1\leq k<p$, if the prime p is greater than 2, $\nu_p\left(\binom{p}{k}(py)^k\right)>2+\nu_p(y)$ when $2\leq k\leq p$. Since $\nu_p\left(\binom{p}{1}(py)\right)=2+\nu_p(y)$, it follows that $\nu_p(s^p-1)=2+\nu_p(y)$. However, $\nu_p(s-1)=1+\nu_p(y)$. As a result, for $p>2$ and $\ell=1+\nu_p(y)$, we have $\lambda(\ell+1,p,s)=\lambda(\ell,p,s)=p$. However, this implies that $\nu_p(\mathrm{ord}_{p^{\ell+1}}(s))=2$, and thus $\alpha_{s,p}=\ell=\nu_p(s-1)$. A straightforward argument now shows the following result:

Proposition 3.11. *Let s be a positive integer and p be a prime divisor of $s-1$. Then*

(1) *If $p > 2$, then*

$$\nu_p(ord_{p^\ell}(s)) = \begin{cases} 0 & \ell \leq \nu_p(s-1) \\ \ell - \nu_p(s-1) & \ell > \nu_p(s-1). \end{cases}$$

(2) *If $p = 2$, then*

$$\nu_2(ord_{2^\ell}(s)) = \begin{cases} 0 & \ell \leq \nu_2(s-1) \\ 1 & \nu_2(s-1) < \ell \leq \nu_2(s^2-1) \\ 1 + \ell - \nu_2(s^2-1) & \ell > \nu_2(s^2-1). \end{cases}$$

Now, suppose that $g = p_1^{j_1} \dots p_n^{j_n}$ with each p_i prime (and $j_i \geq 1$) is defined as in Proposition 3.2. For a given k with $\gcd(k, gs) = 1$, we now determine for which values of $t_1, \dots, t_n$ we have that $p_1^{t_1} \dots p_n^{t_n} k$ are (s,t)-distinguished.

Proposition 3.12. *Suppose $s > t > 0$ are integers, and let g be defined as above with $g = p_1^{j_1} \dots p_n^{j_n}$ the prime factorization of g. Then $p_1^{t_1} \dots p_n^{t_n} k$ is (s,t)-distinguished if and only if for each $i = 1, \dots, n$, the power t_i satisfies one of the following:*

(1) $j_i + t_i \leq \nu_{p_i}(s-1)$,
(2) $p_i = 2$ *and* $\nu_2(s-1) < t_i < t_i + j_i \leq \nu_2(s^2-1)$, *or*
(3) $ord_{p_i^{t_i+j_i}}(s)$ *divides* $ord_k(s)$.

Proof. Since $\mathrm{ord}_p(s) = 1$, the above follows from Lemma 3.5. □

To demonstrate Proposition 3.12 in practice, we consider the case where $(s,t) = (11,1)$. In the following three matrices, the (i,j)-entry represents the whether or not $2^i 5^j k$ is distinguished, where $k = 51, 101$, and 151, respectively. Here $g = p_1^{j_1} \cdot p_2^{j_2}$ where $p_1 = 2$, $p_2 = 5$, and $j_1 = j_2 = 1$. We note that $\nu_2(s^2-1) = \nu_2(120) = 3$, $\nu_2(s-1) = \nu_2(10) = 1$ and $\nu_5(s-1) = \nu_5(10) = 1$, while $\mathrm{ord}_{51}(11) = 2^4$, $\mathrm{ord}_{101}(11) = 2^2 5^2$, and $\mathrm{ord}_{151}(11) = 3 \cdot 5^2$. Computing we obtain the following three charts, where a 'y' denotes that $2^i 5^j k$ is $(11,1)$-distinguished and an 'n' denotes that it is not.

i\j	0	1	2	3	4	5	6
0	y	n	n	n	n	n	n
1	y	n	n	n	n	n	n
2	y	n	n	n	n	n	n
3	y	n	n	n	n	n	n
4	y	n	n	n	n	n	n
5	y	n	n	n	n	n	n
6	n	n	n	n	n	n	n

$k = 51$

i\j	0	1	2	3	4	5	6
0	y	y	y	n	n	n	n
1	y	y	y	n	n	n	n
2	y	y	y	n	n	n	n
3	y	y	y	n	n	n	n
4	n	n	n	n	n	n	n
5	n	n	n	n	n	n	n
6	n	n	n	n	n	n	n

$k = 101$

i\j	0	1	2	3	4	5	6
0	y	y	y	n	n	n	n
1	n	n	n	n	n	n	n
2	y	y	y	n	n	n	n
3	n	n	n	n	n	n	n
4	n	n	n	n	n	n	n
5	n	n	n	n	n	n	n
6	n	n	n	n	n	n	n

$k = 151$

In fact, since either $\nu_2(s-1) = 1$ or $\nu_2(s+1) = 1$, an easy argument shows that such a chart will always have at most one "gap" from a shaded rectangle.

4. Another Spanning Set for $\phi_{s,t}$

As seen in Theorem 1.2, the functions of the form $\psi_{s,t,r,n}$ together with $1/(1-x)$ span the vector space of rational functions fixed by $\phi_{s,t}$. In this section, we generate another spanning set for this vector space.

Consider the map $\rho_{s,t} : \mathbb{Z}_r \to \mathbb{Z}_r$ given by $n \mapsto sn + t \mod r$. Given $n, r \in \mathbb{N}$ with $r \geq 1$ such that r and s are relatively prime, define

$$F_{s,t,r,n} = \{\rho_{s,t}^{(i)}(n) \bmod r : i \in \mathbb{Z}\}, \tag{4.1}$$

where $\rho_{s,t}^{(i)}$ represents the i-th iterate of the function $\rho_{s,t}$.

Define $\Upsilon_{s,t,r}$ to be a complete collection of coset representatives (all chosen to be less than r); i.e., for all $n \in \mathbb{N}$, there exists a unique $n' \in \Upsilon_{s,t,r}$ such that $F_{s,t,r,n} = F_{s,t,r,n'}$. For $r \geq 1$, define

$$\mathcal{F}_{s,t,r,n}(x) = \frac{1}{1-x^r} \sum_{j \in F_{s,t,r,n}} x^j. \tag{4.2}$$

For example, consider the case when $s = 3, t = 1, r = 13$. Then we have the following cosets: $F_{3,1,13,0} = \{0, 1, 4\}, F_{3,1,13,2} = \{2, 7, 9\}, F_{3,1,13,5} = \{3, 10, 5\}, F_{3,1,13,6} = \{6\}$, and $F_{3,1,13,8} = \{8, 12, 11\}$. This produces the following rational functions:

$$\begin{aligned}
\mathcal{F}_{3,1,13,0} &= \frac{1}{1-x^{13}}\left(1 + x + x^4\right) \\
\mathcal{F}_{3,1,13,2} &= \frac{1}{1-x^{13}}\left(x^2 + x^7 + x^9\right) \\
\mathcal{F}_{3,1,13,3} &= \frac{1}{1-x^{13}}\left(x^3 + x^{10} + x^5\right) \\
\mathcal{F}_{3,1,13,6} &= \frac{1}{1-x^{13}}\left(x^6\right) \\
\mathcal{F}_{3,1,13,8} &= \frac{1}{1-x^{13}}\left(x^7 + x^8 + x^{11}\right)
\end{aligned}$$

It is clear by the definition of the map $\rho_{s,t}$ that each rational function of the form $\mathcal{F}_{s,t,r,n}$ is fixed by $\phi_{s,t}$

Theorem 4.1. *Suppose $s \geq 2$ and $1 \leq t \leq s-2$. The collection of all $\mathcal{F}_{s,t,r,n}$ where r is distinguished with respect to (s,t) and $n \in \Upsilon_{s,t,r}$ spans the set of all rational functions that are fixed under the transformation $\phi_{s,t}$.*

Proof. It is shown in [5] (see the proof of Proposition 3.2 in that paper) that for any rational function fixed by $\phi_{s,t}$

(i) the degree of the numerator is less than the degree of the denominator,
(ii) the poles must be simple, and
(iii) the poles must be roots of unity.

Therefore, any rational function fixed by $\phi_{s,t}$ can be expressed in the form $p(x)/(1-x^r)$ where $\deg p(x) < r$.

If $p(x)/(1-x^r) = \sum a_n x^n$ is fixed by $\phi_{s,t}$, then for each $n \in \mathbb{N}$, $a_n = a_{sn+t}$. Therefore, if $j_1, j_2 \in F_{s,t,r,n}$, then $a_{j_1} = a_{j_2}$. This means that coefficients are constant over terms indexed by any given coset $F_{s,t,r,n}$, and so $p(x)/(1-x^r)$ must be a linear combination of rational functions of the form $\mathcal{F}_{s,t,r,n}$. □

It appears that there is a great deal of redundancy in this spanning set. We note that for any choice of s, t, r, N, a, $\mathcal{F}_{s,t,r,N}$ is a linear combination of functions of the form $\mathcal{F}_{s,t,ar,n}$, $n \in \mathbb{N}$. In general, there appears to be a correspondence between functions of the form $\mathcal{F}_{s,t,r,n}$ and $\mathcal{F}_{s,t,ar,n'}$ for appropriate choices of n and n'. It would be nice to see future investigations shed light on the nature of this correspondence.

At this juncture, we pose the question of how to write these two collections of rational functions relate to one another. In particular, we write each function of the form $\psi_{s,t,r,n}$ in terms of functions of the form $\mathcal{F}_{s,t,r,n}$. Consider the example we began with $(s,r) = (3,13)$. Then we have the following cosets: $C_{3,13,0} = \{0\}, C_{3,13,1} = \{1,3,9\}, C_{3,13,2} = \{2,6,5\}, C_{3,13,4} = \{4,12,10\}$, and $C_{3,13,7} = \{7,8,11\}$. This produces the following rational functions:

$$\psi_{3,1,13,0} = \frac{1}{1-x}$$

$$\psi_{3,1,13,1} = \frac{(e^{\frac{8\pi i}{13}} + 1 + e^{\frac{2\pi i}{13}}) + (e^{\frac{5\pi i}{13}} + e^{-\frac{7\pi i}{13}} + e^{\frac{7\pi i}{13}} + e^{-\frac{3\pi i}{13}} + e^{\frac{\pi i}{13}} + e^{-\frac{9\pi i}{13}})x + (e^{-\frac{4\pi i}{13}} + e^{-\frac{2\pi i}{13}} + e^{-\frac{10\pi i}{13}})x^2}{(1-e^{-\frac{8\pi i}{13}}x)(1-e^{\frac{2\pi i}{13}}x)(1-e^{\frac{6\pi i}{13}}x)}$$

$$\psi_{3,1,13,2} = \frac{(e^{-\frac{10\pi i}{13}} + e^{\frac{4\pi i}{13}} + 1) + (e^{\frac{7\pi i}{13}} + e^{-\frac{5\pi i}{13}} + e^{-\frac{3\pi i}{13}} + e^{-\frac{1\pi i}{13}} + e^{\frac{\pi i}{13}} + e^{-\frac{11\pi i}{13}})x + (e^{-\frac{8\pi i}{13}} + e^{\frac{6\pi i}{13}} + e^{-\frac{4\pi i}{13}})x^2}{(1-e^{\frac{4\pi i}{13}}x)(1-e^{\frac{10\pi i}{13}}x)(1-e^{\frac{12\pi i}{13}}x)}$$

$$\psi_{3,1,13,4} = \frac{(e^{\frac{6\pi i}{13}} + e^{\frac{8\pi i}{13}} + 1) + (e^{\frac{7\pi i}{13}} + e^{\frac{11\pi i}{13}} + e^{\frac{\pi i}{13}} + e^{-\frac{11\pi i}{13}} + e^{\frac{3\pi i}{13}} + e^{-\frac{9\pi i}{13}})x + (e^{-\frac{8\pi i}{13}} + e^{\frac{10\pi i}{13}} + e^{\frac{12\pi i}{13}})x^2}{(1-e^{-\frac{2\pi i}{13}}x)(1-e^{-\frac{6\pi i}{13}}x)(1-e^{\frac{8\pi i}{13}}x)}$$

$$\psi_{3,1,13,7} = \frac{(1 + e^{\frac{\pi i}{13}} + e^{\frac{4\pi i}{13}}) + (e^{-\frac{11\pi i}{13}} + e^{\frac{3\pi i}{13}} + e^{\frac{5\pi i}{13}} + e^{\frac{7\pi i}{13}} + e^{\frac{9\pi i}{13}} + e^{\frac{-3\pi i}{13}})x + (e^{-\frac{2\pi i}{13}} + e^{\frac{12\pi i}{13}} + e^{\frac{8\pi i}{13}})x^2}{(1-e^{-\frac{4\pi i}{13}}x)(1-e^{-\frac{10\pi i}{13}}x)(1-e^{-\frac{12\pi i}{13}}x)}$$

Since the functions of the form $\mathcal{F}_{s,t,r,n}$ span the collection of all fixed points of $\phi_{s,t}$ that correspond to the distinguished number r, we can write each $\psi_{s,t,r,m}$ as a linear combination of such functions; that is,

$$\psi_{s,t,r,n_i} = \sum \lambda_{ij} \mathcal{F}_{s,t,r,m_j}$$

for an appropriate choice of constants $\lambda_{ij} \in \mathbb{C}$, where

$$n_1 = 0,\ n_2 = 1,\ n_3 = 2,\ n_4 = 4,\ n_5 = 7$$

and

$$m_1 = 0,\ m_2 = 2,\ m_3 = 3,\ m_4 = 6,\ m_5 = 8.$$

Below is a change of basis matrix M whose (i,j)-entry is λ_{ij}.

$$\left[\begin{array}{ccccc}
\frac{1}{1+e^{\frac{2i\pi}{13}}+e^{\frac{8i\pi}{13}}} & \frac{1}{e^{\frac{4i\pi}{13}}+e^{-\frac{8i\pi}{13}}+e^{-\frac{12i\pi}{13}}} & \frac{1}{e^{-\frac{6i\pi}{13}}+e^{\frac{6i\pi}{13}}+e^{\frac{10i\pi}{13}}} & \frac{1}{3e^{\frac{12i\pi}{13}}} & \frac{1}{e^{-\frac{2i\pi}{13}}+e^{-\frac{4i\pi}{13}}+e^{-\frac{10i\pi}{13}}} \\
\frac{1}{1+e^{\frac{4i\pi}{13}}+e^{-\frac{10i\pi}{13}}} & \frac{1}{e^{\frac{2i\pi}{13}}+e^{\frac{8i\pi}{13}}+e^{\frac{10i\pi}{13}}} & \frac{1}{e^{-\frac{6i\pi}{13}}+e^{-\frac{12i\pi}{13}}+e^{\frac{12i\pi}{13}}} & \frac{1}{3e^{-\frac{2i\pi}{13}}} & \frac{1}{e^{-\frac{4i\pi}{13}}+e^{\frac{6i\pi}{13}}+e^{-\frac{8i\pi}{13}}} \\
\frac{1}{1+e^{\frac{6i\pi}{13}}+e^{\frac{8i\pi}{13}}} & \frac{1}{e^{\frac{4i\pi}{13}}+e^{-\frac{6i\pi}{13}}+e^{-\frac{10i\pi}{13}}} & \frac{1}{e^{-\frac{2i\pi}{13}}+e^{\frac{2i\pi}{13}}+e^{-\frac{12i\pi}{13}}} & \frac{1}{3e^{-\frac{4i\pi}{13}}} & \frac{1}{e^{-\frac{8i\pi}{13}}+e^{\frac{10i\pi}{13}}+e^{\frac{12i\pi}{13}}} \\
\frac{1}{1+e^{\frac{4i\pi}{13}}+e^{-\frac{12i\pi}{13}}} & \frac{1}{e^{\frac{2i\pi}{13}}+e^{-\frac{4i\pi}{13}}+e^{-\frac{6i\pi}{13}}} & \frac{1}{e^{-\frac{8i\pi}{13}}+e^{-\frac{10i\pi}{13}}+e^{\frac{10i\pi}{13}}} & \frac{1}{3e^{\frac{6i\pi}{13}}} & \frac{1}{e^{-\frac{2i\pi}{13}}+e^{\frac{8i\pi}{13}}+e^{\frac{12i\pi}{13}}}
\end{array}\right]$$

Note that the constant coefficients of the $\psi_{3,1,13,n}$ match the first column of M, which is to be expected (and whose justification is left to the reader). However, somewhat surprising is the fact that the coefficients of x^2 in the numerators of each $\psi_{3,1,13,n}$ appear as the entries of the last column of M. We pose the question concerning whether such a correspondence holds in general.

Note that each entry of this matrix is a sum of three or fewer thirteenth roots of unity. At this point, we represent the entries of this matrix in a different fashion. For each thirteenth root of unity that appears, rewrite it in the form $e^{\frac{2ai\pi}{13}}$ where $0 \leq a \leq 12$. For example, $1+e^{\frac{4i\pi}{13}}+e^{-\frac{12i\pi}{13}}$ can be written as $e^{\frac{0i\pi}{13}}+e^{\frac{4i\pi}{13}}+e^{\frac{14i\pi}{13}}$. Then we note each integer a such that $e^{\frac{2ai\pi}{13}}$ is a summand in the given expression. Continuing with our same example, we write $\{0,2,7\}$. Applying this process to the entire matrix M, we obtain the following matrix.

$$M' = \left[\begin{array}{ccccc}
\{0\} & \{0\} & \{0\} & \{0\} & \{0\} \\
\{0,1,4\} & \{2,9,7\} & \{10,3,5\} & \{6\} & \{12,11,8\} \\
\{0,2,8\} & \{1,4,5\} & \{10,7,6\} & \{12\} & \{11,3,9\} \\
\{0,3,4\} & \{2,10,8\} & \{12,1,7\} & \{11\} & \{9,5,6\} \\
\{0,2,7\} & \{1,11,10\} & \{9,8,5\} & \{3\} & \{12,4,6\}
\end{array}\right]$$

It is interesting to note that the entire matrix M' can be easily obtained by scaling cosets of the form $F_{3,1,13,m}$. In particular to obtain the (i,j)-entry of M', consider multiplying the entries of the coset $F_{3,1,13,m_j}$ by n_i and then reduce modulo 13. For example, consider the $(5,3)$ entry of M', which is $\{9,8,5\}$ according to the table above. We note that this entry could have been obtained by multiplying $F_{3,1,13,m_3} = F_{3,1,13,3} = \{3,10,5\}$ by $n_5 = 7$ and then reducing modulo 13. An interesting open question is whether this sort of pattern holds in general.

Let us consider what would have happened if we chose different coset representatives other than $n_1 = 0, n_2 = 1, n_3 = 2, n_4 = 4, n_5 = 7$. For example, suppose we choose $n_5 = 8$. Multiplying each $F_{3,1,13,m_i}$ by $n_5 = 8$ and reducing modulo 13, we obtain the following sets: $\{0,6,8\}, \{4,7,3\}, \{11,2,1\}, \{9\}, \{5,10,12\}$. Note that if add 7 to each of the cosets and reduce modulo 13 we obtain the last row of M', which simply amounts to multiplying the last row of M by a scalar multiple.

The inverse matrix M^{-1} also consists of entries that are sums of roots of unity. However, we have not found a similar type of pattern as M has. It would be interesting to investigate the inverse matrix more fully.

References

[1] G. Boros, J. Little, V. Moll, E. Mosteig, R. Stanley, A map on the space of rational functions, *Rocky Mountain Journal of Mathematics*. **35** (2005), 1861–1880.

[2] G. Boros, V. Moll, Landen transformations and the integration of rational functions, *Mathematics of Computation*. **71** (2002), 649–668.

[3] J. Gil, S. Robins, Hecke operators on rational functions. I., *Forum Mathematicum*. **17** (2005), no. 4, 519–554.

[4] E. Grosswald, *Topics from the Theory of Numbers*, Macmillan, 1966.
[5] E. Mosteig, Fixed Points on the Space of Rational Functions, *Online Journal of Analytic Combinatorics*. **1** (2006).

Department of Mathematics, Loyola Marymount University, Los Angeles, CA 90045
E-mail address: cbennett@lmu.edu

Department of Mathematics, Loyola Marymount University, Los Angeles, CA 90045
E-mail address: emosteig@lmu.edu